beneficiaries of fraud perpetrators' actions. Therefore, it is particularly important that the Commission establish rules that will encourage LECs to participate more actively in the prevention of payphone fraud, as well as rules that will fairly apportion liability to the LECs to the extent that their actions allowed such fraud to occur.

AT&T recommends that the Commission affirmatively establish rules defining carriers' public duty to take reasonable measures to prevent payphone fraud. In particular, AT&T proposes the following guidelines that should be used to apportion carriers' (including PPOs') obligations to prevent, and to assume financial responsibility for, payphone fraud. However, consistent with the principles described in Section II above, each of the proposed rules concerning financial liability should be rebuttable if the carrier presumed to be responsible can prove that another carrier's acts or omissions created the circumstances which allowed the fraud to occur.

### A. PPOs Should Be Initially Liable to IXCs for All Direct-Dialed Calls Placed from Their Telephones and Obtain Recourse When Appropriate from LECs

The Commission has recognized that PPOs generally have the ability to protect themselves against fraud

resulting from calls dialed directly from their payphones.[25] 1+ calls can be blocked by intelligence in the phone or in associated CPE.[26] Calls outpulsed using the 10XXX1+ code can also be blocked by CPE, and in some cases such calls can be blocked in LEC central offices.[27] Further, the Commission has required LECs to provide services capable of blocking international calls dialed using the 011+ or 10XXX011+ codes.[28]

The Commission's decisions in United Artists and similar cases have decided disputes between IXCs and PPOs over payphone fraud based upon technical interpretations of IXC tariff language and determinations of whether PPOs have

---

[25] Policies and Rules Concerning Operator Service Access and Pay Telephone Compensation (Report and Order and Further Notice of Proposed Rulemaking), CC Docket No. 91-35 ("CC Docket No. 91-35"), released August 9, 1991, ¶ 14.

[26] In most cases, PPOs intend (or are required) to allow 1+ calls, and they typically derive revenues from such traffic.

[27] Because private payphones often have the ability to translate customer-dialed numbers into other numbers, the determination of the codes used for a particular call must be based upon the digits out-pulsed from the phone, rather than the digits entered by the caller.

[28] CC Docket No. 91-35, Order on Reconsideration, released July 20, 1992, ¶ 20. That order also requires LECs to provide services that block international calls from the U.S. to foreign locations using the 01+ access code, which is used for outbound international operator services calls.

"constructively" ordered service and thus become customers under the IXC's tariff. AT&T suggests that a better way to resolve these disputes is to recognize the respective ability of the parties -- PPOs, LECs and IXCs -- to control the fraud. This would eliminate the potentially "illogical" disputes over the definition of the term "customer,"[29] and focus attention upon the most important issues: whether the respective carriers have imposed unreasonable risks of toll fraud upon each other, and whether they have complied with their public policy-mandated duty to employ appropriate measures to control toll fraud.[30]

Some PPOs have previously argued that they should be entitled to a "safe harbor" protecting them against liability for fraudulent direct-dialed calls if they merely order appropriate LEC blocking services.[31] AT&T agrees that PPOs should be required to order such services, or be responsible for any IXC fraud losses which result from their

---

[29] See NPRM ¶ 29.

[30] Adoption of such rules would also have the benefit of placing all payphones on an equal footing with respect to toll fraud. For purposes of the discussion below, LECs and other carriers who place public telephones should be obliged to take the same fraud precautions as PPOs in order to avoid liability in their role as a payphone provider. Thus, LECs would be responsible for both ordering and implementing blocking and screening services in order to avoid liability for fraudulent calls involving their own payphones.

[31] See NPRM, ¶ 28.

failure to do so.[32] However, the inquiry should not end at this point. Rather, the Commission's fraud rules should recognize that IXCs have no practical way to prevent or block direct-dialed calls that are later determined to be fraudulent. The rules should thus provide that PPOs have the initial responsibility for fraudulent direct-dial calling from their phones, but that the LECs should bear the ultimate financial responsibility if the failure of a LEC's services is the cause of specific payphone fraud. Such a rule will ensure that IXCs are not held hostage financially while PPOs and LECs dispute liability issues between themselves.[33]

---

[32] PPOs should also be responsible for protecting their phones against "clip on" fraud, which can occur if the wires serving their phones are exposed and unshielded.

[33] Possible disputes over liability between PPOs and LECs are not limited to issues relating to the LEC's provision of blocking services. These parties may argue, for example, whether clip-on fraud occurred on the PPO's or the LEC's side of the demarcation point, and which party had the obligation to provide security at the point the fraud was committed. IXCs are innocent bystanders to such disputes. They should not be required to endure economic loss while those disputes are pending.

B. PPOs Who Comply with Reasonable Fraud Protection Requirements Should Be Relieved of Liability for Fraudulent Operator Services Calls.

PPO payphones, LEC networks and IXC networks interact differently when calls are dialed using operator services access codes.[34] In particular, IXCs should have the ability to protect themselves against such fraud if they receive ANI II screening digits from the LECs. As a result, the Commission's fraud rules should appropriately recognize these facts in applying the liability principles described above.

1. Domestic Calls.

LEC screening services are essential to the prevention of payphone fraud on domestic operator services calls. LEC screening data enable IXCs to know that calls are being placed from, or being billed to, payphones. Therefore, the Commission has appropriately required LECs to participate in fraud prevention efforts by offering originating line screening (OLS) and billed number screening (BNS) services, on an unbundled basis and at reasonable rates.[35]

---

[34] Examples of such codes are 0+, 0-, 00, 10XXX0+, 10XXX0-, 950-XXXX numbers and 800 numbers identified as access codes.

[35] See CC Docket No. 91-35, Order on Further Reconsideration and Further Notice of Proposed Rulemaking, released April 9, 1993, ¶ 16. These services should be provided

(footnote continued on following page)

Because IXCs are able to recognize and act upon LEC screening data, PPOs should generally be entitled to rely upon LEC screening services if they have ordered them in time to be effective before the alleged fraud has occurred.[36] PPOs who timely order such services, keep them in effect, and take reasonable precautions to insure their continued effectiveness should therefore be relieved of liability for fraudulent domestic IXC operator services calls billed to their payphones.[37]

IXCs can participate in payphone fraud prevention by equipping themselves to receive and process the ANI II digits which LECs generate in providing BNS and OLS. Therefore, it is appropriate to hold IXCs financially responsible for fraud on domestic operator services calls

---

(footnote continued from previous page)

separately on an interstate basis, in order to assure that the FCC has jurisdiction to resolve disputes involving interstate fraud. This is particularly important because the value of fraud losses on interstate calls substantially exceeds the losses sustained on intrastate calls.

[36] PPOs, of course, must also order access lines from LECs that are specifically designated as payphone lines. Otherwise, there is no assurance that IXCs' ability to recognize OLS signals will protect the PPOs from being billed for calls originating at their payphones.

[37] Appendix D provides a list of actions that PPOs should be required to perform during installation and regular maintenance to assure that the LEC screening services are working properly.

billed to payphone lines if they have received the ANI II screening digits from the originating LEC. If, however, an IXC can demonstrate from its AMA call records or other data that the LEC did not properly transmit the ANI II screening digits, the LEC should be responsible to the IXC for the latter's charges on fraudulent calls from private payphones.

2. International Calls.

The Commission's discussion of international payphone fraud focuses specific concern upon collect calls that originate in foreign locations and are billed to payphones in the United States ("in-collect" calls). The NPRM (¶ 27) notes that the FPSC has suggested that foreign telephone service providers ("PTTs") should be required to launch BNS inquiries on such calls.[38] This suggestion could be unworkable, however, because of the uncertainty of applying and enforcing such a rule extra-territorially and because it is highly unlikely, in any case, that all PTTs could make their own operator systems compatible with the LECs' LIDB data bases within a reasonable period of time.

There is, however, another way in which such fraud can be reduced and responsibility could reasonably be shared. Some IXCs, including AT&T, have made arrangements

---

[38] Such queries would determine whether the party responsible for the called telephone wishes to block all collect calls to that phone.

for PTTs to inform them of all in-collect calls billed to telephone line numbers whose last four digits are in the 8000-9999 range. LECs typically assign such telephone numbers to their own public telephones. In such cases, the IXC can perform a LIDB query and deny the call if the called telephone subscribes to BNS.[39] Some LECs, such as Pacific Bell, have already been helpful in assigning line numbers in the 8000-9999 range to private payphones as well. A Toll Fraud Prevention Commottee Resolution in 1991 urged that line numbers for all payphones be assigned (or reassigned) in the 8000-9999 range where practicable, and AT&T knows of no reason why such number assignments would not be possible. AT&T therefore proposes that all LECs be required promptly to implement the TFPC Resolution, and PPOs be required to order and accept such numbers.

---

[39] AT&T has already instituted a policy of querying LIDB on foreign in-collect charges billed to phones whose line numbers are in the 8000-9999 range.

C. Limitations of Liability in LEC Tariffs Should Not Prevent an Equitable Sharing of the Financial Responsibilities for Toll Fraud.

The Commission (NPRM ¶ 31) "finds merit" in the FPSC's proposal that the Commission "review those portions of tariffs filed with the Commission that limit carrier liability associated with payphone fraud." AT&T concurs, especially with respect to LEC tariffs that purport to limit their liability in connection with blocking and screening services.

The blocking and screening services which the Commission has required the LECs to provide are designed solely to prevent fraudulent calls. Indeed, these services are the single most important means of enabling PPOs, IXCs and their customers to be protect themselves from a large proportion of payphone fraud. Thus, unlike the general limitation of liability in carriers' tariffs, a limitation on liability for fraudulent calling for a tariffed service designed solely to prevent fraud could thwart the Commission's public interest objectives in requiring such services to be provided.[40]

---

[40] The rules AT&T suggests would not, however, affect the LECs' (or any other carrier's) right to protect themselves with a tariffed limitation upon their liability for consequential damages, i.e., indirect damages such as lost profits suffered by an end user customer. Rather, these rules should address only liability for "direct" damages, i.e., the tariffed charges for fraudulent calls.

Furthermore, the vast preponderance of payphone fraud consists of interstate (and particularly international) calls, providing the LECs with little economic incentive to maintain the quality and reliability of their vital blocking and screening services. In fact, as noted above, the LECs' access charge revenue stream could be viewed as inconsistent with careful provision of such services. Holding the LECs responsible for the fraud which results from failures of these blocking and screening services would provide the LECs with appropriate incentives to increase the effectiveness of such services and thereby reduce the likelihood of fraud.

In sum, adoption of AT&T's proposals will provide all of the involved carriers with significant incentives to implement effective fraud reduction measures. This, in turn, will benefit all consumers by reducing the costs associated with payphone fraud.

## IV. CELLULAR CARRIERS SHOULD BE RESPONSIBLE FOR IXC FRAUD CAUSED BY CLONING.

Part D of the NPRM requests comments on actions the Commission should take to help reduce fraud associated with the use of cellular telephones. The NPRM (¶ 33) recognizes three basic types of cellular fraud: subscription fraud, fraud resulting from the use of stolen phones, and access fraud, but inquires principally about access fraud. With respect to access fraud caused by "tumbling", the

Commission (NPRM ¶ 33) correctly notes that the cellular industry has appropriate incentives and is making significant strides to improve validation technology that will reduce such losses.

The Commission (NPRM ¶ 34) notes that it has already proposed technical rules that should lead to a prospective reduction in access fraud caused by "cloning" for future generations of cellular phones.[41] AT&T supports the adoption of rules that would make it more difficult to alter newly manufactured cellular handsets so that they copy valid Electronic Serial Number/Mobile Identification Number combinations. Such actions, however, will not affect or reduce losses that result from the fraudulent cloning of existing cellular telephones.

Under the liability principles described above, liability for fraudulent IXC network calls from cloned phones appropriately rests upon the cellular carriers who allow such calls to reach the IXC networks.[42] IXCs have no practical way to detect whether calls are made from

---

[41] See Revision of Part 22 of the Commission's Rules governing the Public Mobile Service (Notice of Proposed Rulemaking), 7 F.C.C. Rcd. 3658, 3741 (1992).

[42] This is particularly true for non-wireline cellular carriers who purchase IXC services in bulk and provide bundled cellular/IXC services. These carriers are themselves ordering service in their own name from IXCs and should pay for all services provided.

telephones using authorized ESN/MIN combinations or from phones which have been fraudulently cloned. Moreover, unlike cellular carriers, whose principal "losses" are for airtime on their own networks, IXCs have substantial out-of-pocket costs associated with such calls, including access charges and billing and collection expenses, as well as settlements payments on international calls.

In all events, the costs of cloning fraud result solely from the use of cellular technology. Therefore, the costs of such fraud should be borne by the cellular carriers and their subscribers who use that technology, rather than IXCs and their customers. The Commission should thus adopt rules that make the cellular carriers responsible for IXC charges that result from cloning fraud. These rules will also provide economic incentives to such carriers to develop and implement technical means to control such fraud.

## V. CARRIERS WHO ATTEMPT TO QUERY LIDB ON A CALL CHARGED TO A LEC JOINT USE CARD, AND WHO OFFER TO PROVIDE CALL DETAIL INFORMATION ABOUT SUCH CALL, SHOULD BE REIMBURSED BY THE LEC FOR ANY RESULTING FRAUD LOSSES.

Part D of the NPRM seeks comments on issues relating to fraud generated through the use of LEC joint use calling cards. Information on such cards is stored in line information data bases, or LIDBs, maintained by, or on behalf of card-issuing LECs. Carriers who wish to bill calls to such cards typically query the appropriate LIDB in order to determine whether the card is valid in the issuer's

data base. This is the only validation capability available to such carriers.

Toll fraud associated with use of LEC joint use calling cards is very substantial, amounting to many times the fraud associated with PBX abuses. Moreover, AT&T's fraud experience with LEC card calls is disproportionately high compared to the fraud levels associated with the use of AT&T's own proprietary calling cards. Such experience indicates that LECs may not have sufficient incentives to increase their fraud detection capabilities[43] and that there are a number of additional fraud control measures that the LECs could undertake to increase the reliability of their LIDB systems, especially if they have appropriate information available to them.

AT&T agrees with the Commission's assessment (NPRM ¶ 36) that IXCs should query LIDB each time they consider accepting a LEC card for payment. This information will enable LECs to detect "spikes" of usage on specific cards and can help to control fraudulent usage of LEC cards. Therefore, IXCs should not be permitted to store and reuse

---

[43] As noted in Section II above, LECs collect access charges and LIDB validation charges on fraudulent calls billed to their calling cards.

LIDB validation information for calls they complete over their networks.[44]

AT&T also agrees with the LECs that other carriers should, whenever possible, provide the card issuer (or its LIDB operator) with originating and terminating numbers in connection with validation queries.[45] This would help LIDB operators to improve their fraud detection capabilities, by enabling them determine whether a specific call is originating or terminating in a "high fraud" area, and by developing standard usage patterns for LEC cards.

The Commission (NPRM ¶ 37) further asks whether carriers who provide the above information to the LECs should be entitled to charge for providing it. AT&T

---

[44] Carriers whose own prior experience with specific LEC cards leads them to reject callers' attempts to use those cards need not query LIDB with respect to those cards. However, AT&T recommends that carriers making such decisions should provide the issuing LEC with the usage or attempt data underlying the decision to deny credit. This will assist the LEC in its fraud investigations and its future determinations of whether to allow continued use of the card.

[45] See NPRM, ¶ 37. For domestic calls, IXCs should be able to provide LECs with the ten-digit originating and terminating numbers. For calls originating in the United States and terminating outside of the country, IXCs should be required to provide the country code for the terminating telephone. For calls originating from international locations and terminating in the United States, the IXC should provide an "international" indicator in lieu of the originating number, which in nearly all cases is unknowable.

believes that the appropriate consideration for offering this information should be a right to rely upon the LIDBs themselves. Thus, carriers who launch a LIDB query containing the above information should be indemnified by the LEC against loss of their tariffed charges for any fraudulent call described in the query, unless the LEC provides an "invalid" response within a reasonable period.

This rule has several advantages. First, it is simple to administer and relies upon data that should be available from ordinary call records. Second, it provides LECs with the data they need to increase the reliability of their LIDBs for themselves, all other carriers, and ultimately for customers. Third, it provides appropriate financial incentives to other carriers to provide important information to the LECs.[46] Fourth, it will provide incentives for the LECs "to make LIDB[s] as effective as [they] can be."[47]

As described above, LIDBs are necessary to prevent fraud on calls billed to LEC cards. Therefore, the public's interest in reducing toll fraud would not be served if LECs were allowed to shield themselves from liability if the

---

[46] Carriers who choose not to assist in fraud prevention by fulfilling these requirements should be liable for any fraud on calls they allow.

[47] NPRM ¶ 39.

above conditions are met. The Commission should adopt a rule requiring LECs to assume financial responsibility for fraudulent calls billed to their own calling cards when another carrier offers to query LIDB and provide the call detail information described above.

## VI. THE COMMISSION SHOULD TAKE ADDITIONAL STEPS TO COORDINATE EXISTING INDUSTRY EFFORTS TO REDUCE TOLL FRAUD.

The NPRM also requests comments on ways in which it can facilitate closer coordination among interested parties to reduce toll fraud. In particular, the Commission seeks comments (NPRM ¶ 13) on whether and how it can "add value" to existing inter-institutional fraud reduction efforts and whether it should participate in efforts to encourage new legislation targeted to toll fraud.

### A. The Commission Should Increase Its Participation in Existing Industry Toll Fraud Prevention Groups.

There are already a number of industry efforts aimed at detecting toll fraud problems and reducing toll fraud risks. These institutions include the Toll Fraud Prevention Committee ("TFPC"), the Interexchange Carrier Industry Subcommittee Toll Fraud Subcommittee ("ICICTFS") and the Communication Fraud Control Association ("CFCA").

The industry would benefit from greater Commission participation in those groups.[48] Active Commission participation in these groups could bring additional perspective to their operations and also keep the Commission better informed of fraud prevention activities that are already underway.

AT&T further suggests that the fraud implications of new technologies, especially wireless technologies, make it critical that the industry keep the Commission advised of technical issues relating to fraud. As products are developed to work with new wireless services such as PCS, for example, the Commission needs to be able to develop registration requirements that will provide the maximum possible protections against fraud. This is particularly important for CPE that will be used in connection with unlicensed spectrum applications which enable users to interconnect with the public network. Such efforts are fully consistent with the Commission's commitment (NPRM ¶ 5) to work with the industry to develop solutions to fraud problems "without hindering the development or use of these new technologies." In connection with such efforts, the

---

[48] In order to facilitate such participation, AT&T suggests that these groups make an effort to schedule meetings at times and places convenient for Commission representatives.

Commission should create an industry forum that can address cooperatively these new fraud challenges.

### B. The Commission Should Encourage the Enforcement of Existing Criminal Statutes and the Adoption of More Effective Toll Fraud Prevention Statutes.

The NPRM (¶¶ 3, 12) recognizes that toll fraud is a crime that generates billions of dollars in losses.[49] The Commission (NPRM ¶ 12) correctly notes, however, that there is no specific federal legislation regarding toll fraud, that existing statutes are of "limited effectiveness," and that criminal prosecution of perpetrators is infrequent. Moreover, only a limited number of states have adopted statutes specifically dealing with telephone fraud crimes. All of these deficiencies result in higher costs to consumers.

The Commission can help the industry and consumers to avoid such costs by acting as an advocate for increased enforcement of existing criminal laws and the adoption of new laws -- particularly federal statutes -- that focus upon the specific characteristics of toll fraud. In order to promote the public's interest in reducing such costs, AT&T

---

[49] The amounts involved in each individual instance of fraud are often relatively small. Nevertheless, the aggregate losses resulting from toll fraud are enormous, and they create a substantial burden on carriers, equipment suppliers and their customers.

recommends that the Commission convene a forum of interested parties to develop model legislation that could be implemented at both the federal and state level. In particular, this forum should develop laws which make it a specific crime to use other parties' telecommunications equipment or calling card numbers (or similar codes) for the purpose of making unauthorized telephone calls. In addition, legislation should be developed that would make it a crime for unauthorized persons to possess devices whose principal use is to commit toll fraud. Such devices could include, for example, "red boxes" and "blue boxes" used to place unauthorized calls from public telephones, as well as "listening" devices whose principal purpose is to obtain the electronic serial numbers of cellular telephones.

The Commission should also use its offices to impress upon other Federal government agencies the extent of existing toll fraud and the importance of taking appropriate enforcement action to curb such fraud, including the need for funding to investigate telephone network abuse. Through its coordination with bodies such as NARUC, the Commission should also assist state commissions to achieve the same objectives in their own jurisdictions. Such efforts would not merely benefit members of the telecommunications industry, but also their customers, who ultimately pay for the costs of toll fraud.

## CONCLUSION

The Commission has recognized that toll fraud is a serious and expensive problem that affects the entire spectrum of participants in the telecommunications industry and their customers. Adoption of rules based upon the principles suggested above will enhance the existing incentives to reduce toll fraud and appropriately apportion the financial responsibility for the fraud which occurs.

Respectfully submitted,

AMERICAN TELEPHONE AND TELEGRAPH COMPANY

By _____

Mark C. Rosenblum
Robert J. McKee
Richard H. Rubin

Its Attorneys

Room 3254A2
295 North Maple Avenue
Basking Ridge, New Jersey 07920

Dated: January 14, 1994

# APPENDIX A

## Examples of AT&T Customer Education Materials on Toll Fraud

The attached examples represent a few of the dozens of different customer information packages, bill inserts and news releases on toll fraud prepared by AT&T. Some of the attached items are printed in up to seven languages.

# New Service Offerings Combat Toll Fraud

"We came in Monday morning, and there were $50,000 in fraudulent weekend toll charges on our SMDR printout!" The Telecommunications Manager involved prefers anonymity, but the story is a true one. It's not a record; fraudulent charges measured in hundreds of thousands of dollars over just a few days are not unknown. Toll fraud is a rapidly growing problem, costing U.S. companies over $1billion a year, according to Bob Carmen of AT&T Corporate Security. Calling toll thieves "hackers" understates the seriousness of the problem; theft of communications service is an organized, criminal enterprise these days that we all need to take very seriously.

## HELP FROM AT&T

Where the customer has control over the configuration and use of AT&T products and services, the customer must properly bear the responsibility for fraudulent use of those products and services. However, AT&T recognizes its responsibility to help customers prevent and stop toll fraud. AT&T's support has taken the form of educating and informing customers about security practices through training, security audits, and security tips and security alerts. In addition, AT&T has increased its focus on the development of security systems, as evidenced by the recent announcements of the DEFINITY® System Generic 3 and the HACKER TRACKER™ software designed to detect and deter toll fraud.

**New Security Handbook.** AT&T has summarized the principal steps that should be taken to reduce security risks for all of BCSystems' products in the new 132-page Security Handbook developed by a team of security experts from Bell Labs. It's an invaluable resource, detailing prescriptions for better security. Call the Customer Information Center (800-432-6600) and order 555-025-600; price is $65, or $35 if you're in the CIC Preferred Customer Discount Program.

**New training.** There's also a new Individualized Learning Program (ILP) on security that includes a videotape overview and a series of workbook exercises on risks and how they can be prevented. A copy of the Security Handbook is included with every ILP program. Order the ILP from the CIC, 555-025-601. Price is $125; $95 in the Discount Program.

**Security seminars.** AT&T will be sponsoring free half-day security seminars for customers on a monthly basis starting this fall at locations around the country. For further information, call your AT&T Account Team.

**Electronic services.** The Electronic Information Service (EIS), BCSystems' electronic newsletter, features security tips, ideas, and, in some cases, alerts for customers who subscribe to this free communications service. Valuable security information can be transmitted to EIS users at a minute's notice. And, on June 30, EIS was enhanced to include an Interactive Bulletin Board. This Bulletin Board enables EIS users to share ideas, issues, problems, and solutions regarding security as well as other systems products and topics. AT&T security experts are members of the Bulletin Board — offering insight on a daily basis. To become an EIS user, call 800-242-6005, Department 186.

## SECURITY AUDIT SERVICE

The Security Audit is a fee-based consultative service that provides a security evaluation of a customer's telecommunications system.

The Security Audit is performed by a special team from the Technical Service Center (TSC) in Denver together with security managers from AT&T Network Security. The process starts with a preliminary telephone interview. That's followed by an on-site (or remote) security audit of the equipment followed by an analysis of system vulnerability and written recommendations for increasing security.

Jim Moranor, System Security Audit Manager at the TSC reports, "Our first few audits show customers have a good awareness of security measures. They use the unique Enhanced Call Transfer feature of AUDIX™ Voice Mail Systems and the full set of call-routing features of the DEFINITY System to protect against unauthorized transfer to external trunks. We recommend password security and Remote Port Security Devices to protect against the vulnerability of the remote maintenance port."

To request a Security Audit, call your Customer Service Center (see page 14). The cost of an Audit will depend on the system's complexity. As an example, a stand-alone Generic 1 would average $2,500.

## FRAUD INTERVENTION

The Fraud Intervention Service, provided by the TSC, is a timely response to customers who either are experiencing or suspect fraud. Customers should call 800-242-2121 for immediate and priority assistance. AT&T's commitment is that within two hours of receiving the call, a TSC toll-fraud specialist will work with the customer to:

- Stop the immediate fraud situation.
- Identify the solution and advise the customer of the work required.
- Identify any follow-up work required.

This service is billable and is not covered by the standard service agreements, and solutions offered through this service are limited to correcting the immediate problem.

## AT&T HACKER TRACKER

AT&T HACKER TRACKER software alerts you to abnormal calling activities. You can program the HACKER TRACKER software to monitor incoming calls and watch for hallmarks of hacker activity. It provides alarms and alerts to designated security systems administrators if definable thresholds are exceeded. It's designed to work in conjunction with the Call Accounting System Plus, Version 3. If you have an earlier release of CAS, you can upgrade for a nominal fee.

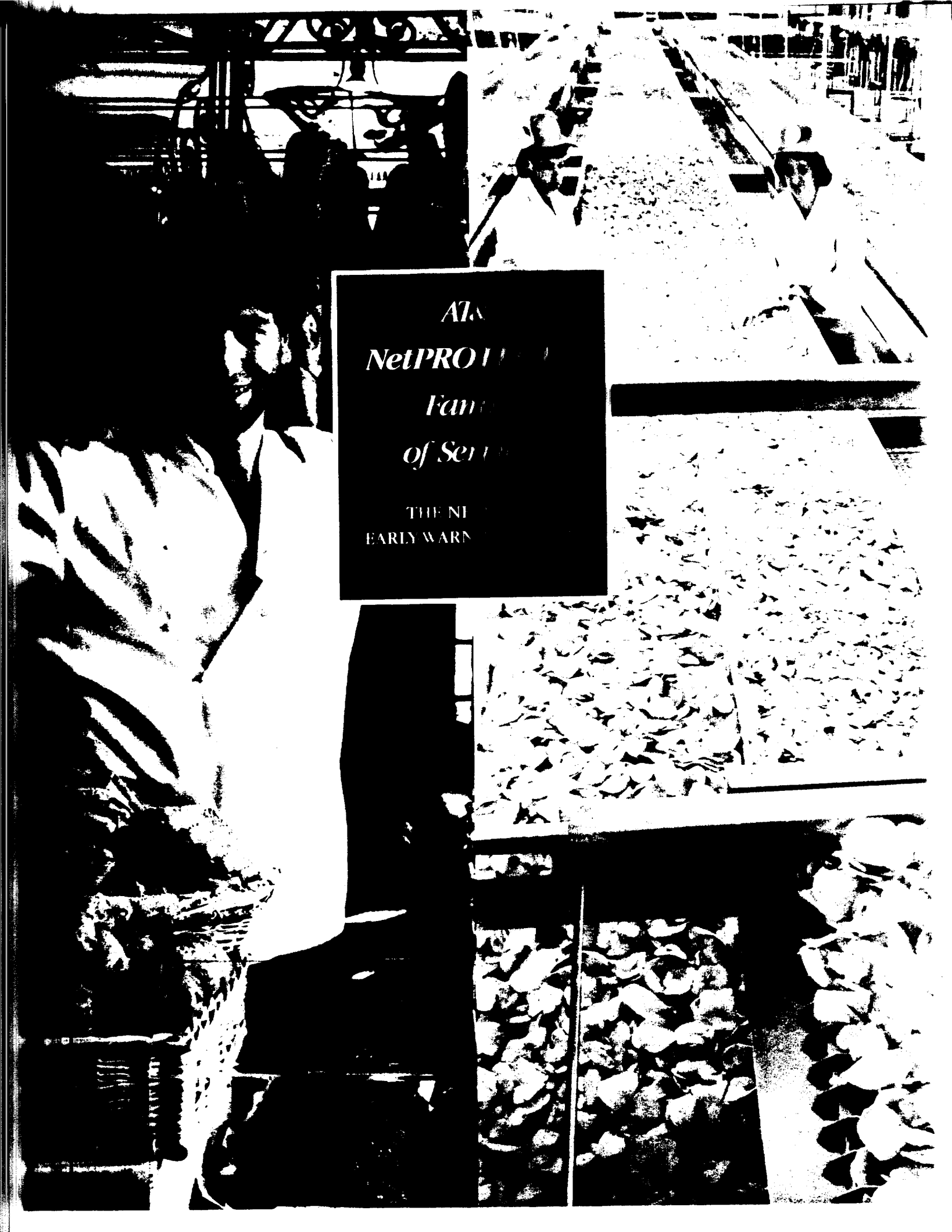
*Your AT&T Account Team can help you fight toll fraud. Call them or call AT&T Corporate Security at 800-821-8235.*

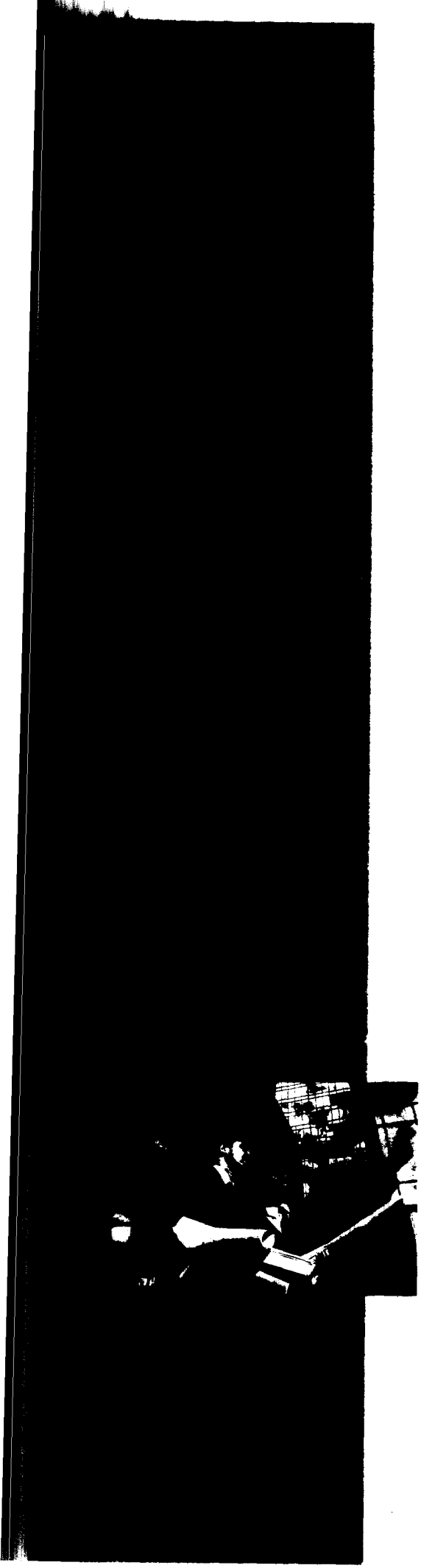
AT&T

*etPROTECT℠*

*y of Services*

NETWORK
ARNING SYSTEM


NetPRO
Fam
of Ser
THE NE
EARLY WARN



# *AT&T NetPROTECT℠ Services* Help Detect and Eliminate Toll Fraud Fast.

According to recent estimates, U.S. businesses lose over $2 billion annually to "telephone hackers" – those technologically sophisticated criminals who use remote means to break into phone systems and run up huge charges in unauthorized calls.

How can companies defend themselves against such high-tech theft? Through awareness. Vigilance. And above all, early detection. And that's why AT&T created the *AT&T NetPROTECT℠ Family of Services* for its customers.

## A VALUE-ADDED BENEFIT OF *AT&T BUSINESS LONG DISTANCE SERVICE* AND *AT&T DOMESTIC 800 SERVICE.*

The *AT&T NetPROTECT℠ Family of Services* is designed to help business customers protect their phone systems against costly toll-fraud losses by providing timely warnings of certain calling patterns that AT&T believes are generally "suspicious." *AT&T NetPROTECT℠ Services* also provide prompt assistance in identifying fraud and valuable information on toll fraud and its prevention. They are available to all AT&T business customers who:

- Own or lease one or more PBX or Single Keypad Systems and
- Subscribe to an *AT&T Business Long Distance Service* and/or *AT&T Domestic 800 Service.*

To accommodate the special needs of different businesses, the *AT&T NetPROTECT℠ Family of Services* provides different levels of service:

## *AT&T NetPROTECT℠ BASIC SERVICE*: AN AUTOMATIC BENEFIT OF CHOOSING AT&T.

Provided to all AT&T business customers at **no additional charge**, *AT&T NetPROTECT℠ Basic Service* brings **added value** to *AT&T Business Long Distance Service* and/or *AT&T Domestic 800 Service* by offering:

- Corporate security monitoring – 24 hours a day, 7 days a week. Monitors the *AT&T Domestic 800 Network* and AT&T outbound direct-dial international calling to over 30 areas known to be "high-fraud destinations." When generally suspicious calling patterns suggesting Remote Toll Fraud are detected, AT&T will quickly attempt to notify the customer.
- Frequent corporate security seminars for each region of the country.
- A basic level of toll-fraud detection service **free of charge** to all customers who have either a PBX or Single Keypad System. That's a valuable benefit for AT&T customers.